FREQUENCY HOPPING USING CDMA TO AVOID MALICIOUS ATTACK IN HAN NETWORKS

HUSSEIN ALI RIDHA

A project report submitted in partial
Fulfillment of the requirement for the award of the
Degree of Master of Electrical Engineering

Faculty of Electrical and Electronic Engineering

Universiti Tun Hussein Onn Malaysia

JANUARY 2020

This Master's Project Report is humbly dedicated to Almighty God, my father

My mother and my wife, my children

Thanks for your endless support!

ACKNOWLEDGEMENTS

First and foremost, praise is to Almighty Allah for all his blessings and for giving me patience and good health throughout the duration of this master's research. Profound appreciation and thanks are also given to my supervisor, Dr. Nik Shahidah Afifi Md Taujuddin for his supervision, guidance, constructive suggestions and comments during the entire research period until its completion. Her advice and support throughout the program have been invaluable. Without her tireless help, leadership and confidence in my ability, the completion of this project would not have been possible. I would also like to thank all post-graduate students of UTHM for their help, friendship and creating a pleasant working environment throughout my study in UTHM. I would like to thank my friends for accepting nothing less than excellence from me. Last but not the least, I would like to thank my family, the reason of my existence: my parents and to my brothers and sisters for supporting me spiritually throughout writing this thesis and my life in general - thank you for being by my side in every step I took during my study.

ABSTRACT

Frequency hopping and Code-Division Multiple Access (CDMA) is often deployed to protect wireless communication from malicious attacks. The data is enabled to be received by the recipients. The data is delayed or blocked when it try to enter the network. This project is developed by hybrid the Frequency Hopping with CDMA in a tangible way to protect the data by giving them an automatic protection. The results have been proved that by hybrid the Frequency Hopping and CDMA shows a better performance in protecting the data compared to the system that just using Frequency Hopping or CDMA only. It has been proved by simulation results that nodes protected by using CDMA and Frequency Hopping will give a better protection with the death nodes will only appears if the nodes are more than 150.

ABSTRAK

Frekuensi Lompatan (FH) dan Kod Pembahagi Capaian Pelbagai (CDMA) sering digunakan untuk melindungi komunikasi tanpa wayar daripada serangan penceroboh. Data ditetapkan untuk diterima oleh penerima. Data juga boleh ditangguh atau disekat apabila ada cubaan untuk masuki rangkaian data. Projek ini dibina dengan menggabungkan Frekuensi Lompatan bersama CDMA dengan cara yang yang tepat serta nyata untuk melindungi data dengan memberi perlindungan secara automatik Keputusan telah membuktikan bahawa gabungan Frekuensi Lompatan dan CDMA adalah jauh lebih baik dari segi prestasi dalam melindungi sistem penghantaran data berbanding prestasi yang ditawarkan oleh sistem yang hanya menggunakan Frekuensi Lompatan atau CDMA sahaja. Melalui simulasi yang dijalankan, didapati nod yang dilindungi menggunakan Frekuensi Lompatan (FH) dan CDMA mempunyai ciri keselamatan yang lebih baik dimana nod mati hanya akan muncul jika jumlah nod melebihi 150.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview of the project

As the value and use of information continues to increase, individuals and businesses seek additional ways to process and store information. One option is an information handling system. An information handling system generally processes, compiles, stores, or communicates information or data for business, personal, or other purposes. Technology and information handling needs and requirements can vary between different applications. Thus information handling systems can also vary regarding what information is handled, how the information is handled, how much information is processed, stored, or communicated, and how quickly and efficiently the information can be processed, stored, or communicated. The variations in information handling systems allow information handling systems to be general or configured for a specific user or specific use such as financial transaction processing, airline reservations, enterprise data storage, or global communications. In addition, information handling systems can include a variety of hardware and software resources that can be configured to process, store, and communicate information and can include one or more computer systems, graphics interface systems, data storage systems, networking systems, and mobile communication systems. Information handling systems can also implement various virtualized architectures. Data and voice communications among information handling systems may be via networks that are wired, wireless, or some combination.

The transmission capacity (ultimate bit rate) of a digital wireless communications system is based on a number of different parameters including (a) total radiated power at the transmitter, (b) the number of antenna elements at the transmitter and receiver, (c) noise power at the receiver, (d) characteristics of the propagation environment, (e) bandwidth, etc. For a wireless transmission system

employing an appreciable number of antennas at both the transmitter and receiver and operating in a so-called Rayleigh fading environment even without coding, the bit rate could be very large, e.g., 36 bits per second per Hz with a reasonable Signal to Noise Ratio (SNR) of 18 dB. Heretofore, it was difficult for a communications system to exchange data at a fraction of such a rate. The main reason for this is that the prior art did not appreciate the problems that had to be solved in order to build a large bit rate system.

For HAN (Home Area Network) system, the network is small. Typical size will be around 100 m x 100 m. The network consists of wireless sensors, hot spot access point and other wireless communication devices. The HAN system is projected for future smart house where all the devices can be access remotely from far distance [3]. Because all the devices that forming the HAN and they can communicate to each other, so there is a need of security to protect the data flows in the network. HAN uses very low data rate and typical communication will use IPv6 (refers to IoT network). The network can be expanded if the number of devices are increase [4].

There are two transparent security systems that can be observed in the CDMA frequency hopping system. One is CDMA itself and second is frequency hopping. The CDMA generates random codes where it helps to protect the data. These codes are embedded into the data frame and will be extracted at the receiver when the receiver successfully recognize the data. The frequency hopping on the other hand provide randomly switches the carrier frequency in order to avoid the malicious attack and avoid other user who uses the same frequency. In the research, it is found that the tendency of frequency hopping scheme generates the frequency, which is similar to other user is very low or it can be said that it never happen or hardly to happen. Therefore, it is safe to use frequency hopping in the wireless communication to enhance the security system [6].

1.2 Problem Statements

Malicious attack is a third party data destroyer who send a harmful packet that can destroy the data in a communication. The cause of malicious attack are:

- Data is unable to be received by the recipients.
- Data being delayed or block when trying to enter into the network.

- A data flow is slow in the network.

There are quite a number of solutions proposed to enhance the network security to avoid the malicious attack. Each solution proposed is unique to overcome the problem of malicious attack. However, the latest research is using the block-chain technology to enhance the network security but this technique has a weakness point because it's using only one frequency channel. Other security scheme like frequency hopping was also employed until today. This is because this scheme is still found useful to avoid the malicious attack [2].

Since the HAN is not a big network, therefore frequency hopping scheme is proposed to enhance the security. The proposed frequency hopping is using Code Division Multiple Access (CDMA) scheme to avoid malicious attack. It is believed that malicious often use. Some sort of frequency to detect the wireless data and hence jam the data transmission or locked into the system in order to destroy the data. By using CDMA frequency hopping scheme, the carrier frequency will be switch randomly. Hence, it is difficult for the malicious to know the exact or fix frequency used in the HAN network [5].

Single frequency used for transmission is very easy to intercept intruder can simply try all the available frequency to steal the information. Hot suitable for high confidential date.

Multiple frequencies are very hard to intercept because it use many frequency. At the receiver, the data is modulated.

1.3 Research Objectives

The objectives of the research are:

i. To develop a CDMA Frequency Hopping Scheme that can prevent the malicious attack in a wireless HAN network.
ii. To analyse the CDMA scheme proposed and show it can protect data frame.
iii. To present the complete CDMA frequency hopping system in a tangible way to protect the data.

1.4 Scope of the Research

The scope of the research will cover the following topics:

1. Use CDMA frequency hopping scheme plays an important role to enhance the security system, two software are used. One is MATLAB and second one is Visual Basic.
2. Use CDMA Frequency Hopping scheme will be developed on Matlab.
3. Use visualization of malicious attack under CDMA frequency Hopping will be done on VB.

The most challenging part is not the theories about the frequency hopping and the CDMA scheme, but is the software implementation of CDMA frequency hopping system. Because learning the MATLAB and Visual Basic is not easy. It may incur many programming, therefore more time will be spend to learn the MATLAB and the Visual Basic.

1.5 Overview of Thesis Arrangement

This report consists of five chapters. These chapters are introduction, literature review, methodology, results & discussion and conclusion & recommendation. Chapter one is an introduction. This chapter introduces overall idea about the CDMA frequency hopping scheme and how it helps to protect the user data in a wireless network HAN. The chapter also shows the objective, problem statements as well as the scope of the research.

Chapter two will present the theories about the CDMA frequency hopping scheme and other related research topics. The chapter will split the discussion between two. One is CDMA and second is frequency hopping. Many related researches where they had published will be presented in this chapter.

Chapter three will present the methodology of implementing the CDMA frequency hopping scheme. This chapter will show the usage of MATLAB and Visual Basic. The design flowchart and the programming coding will be presented in this

chapter. Chapter four will show the results and discussion. This chapter discuss the outcomes after running the simulation.

Chapter five presents the conclusion and recommendation. This chapter concludes the works done in the research summarize the important points about the CDMA frequency hopping against the malicious attack. The chapter also presents some of the suggested ideas to further improve the research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter will present various kinds of communication systems. All are about wireless communications. The communication basically is a sending of information from sender to the receiver from far distance. The information send or received could appears in voice, text, graphics, videos or even animations. To have a communication, there are at least two communication devices exist. Both of these devices are transceivers. Example of communication devices are mobile phone, laptop, personal pager, wireless alert system and so on. As long as any devices which can send any types of signal to the other devices, then we can say the communication is formed.

The communication nowadays is fully digital. If the information signals are appear in analogue, the information signals must converted into digital signals. Thus, in this case there is a need of analogue to digital converter. The communication appears in digital format is convenient to manipulate as the information is using a combination of digital 1 or 0 represent on it. With different arrangement of digital 1 and 0, we will obtain different information. The formation of digital 1 and 0 also can create a secrete code to protect the information. This is usually placed in upfront of all the data. Such protection is called encoder. Apart from the information protection, the formation of digital 1 or 0 also can create an address. The address is important for the digital signal to identify the source and destination [13].

2.2 Types of communications

In this world, the communication systems can be broadly divided into wired communications and wireless communications. The wired communications are using copper wire in the network to send and receive the data. The fibre optic wire is also classified under the wire type of communication. Fibre optic is chosen in the communication because it helps to reduce the noise interference in the communication system as the light source is used to send and receive the digital data.

The fibre optic also have another advantages over the wired types of communications. The advantages of using fibre optic wire apart from avoiding interferences are [14].

1. Provide wide bandwidth in communication
2. High speed data rate
3. Information can be delayed or controlled by making fibre wire into a coil

2.2.1 Wired Communications

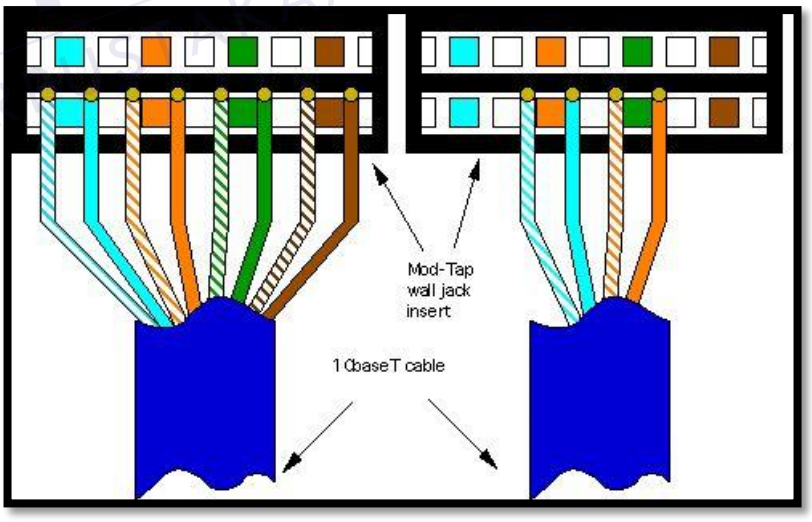


Figure 2.1: TBase copper wires for data communication [15].

The wire types of communication is very common. Since in 18 century, before or just discovered the radio communications, wire communication were used. The wire communication is very stable. It links from one computer to another computer. When more computers exist in a network, the number of wires used will be increased and hence this make the network become complex.

Wire communication using copper as a sole material has a limitation on bandwidth. Apart from that, the cost of making the wire also increased. As the data send in high speed, there is a need to do a new research to release a new wire to support the high speed data communication.

Today we can see a lot of wires communication fall into various types of wires for data communications support. All these wires are designed based on the speed and bandwidth of the data. Example of copper wires for data communication are TBase 10, TBase 100 and TBase 50. All these wires are using LAN port for connection to terminal and entrance of the network. As shows the figure 2.1.

The characteristics of wires are:

1. Twin line
2. Twisted line to cancel the cross-talk effects
3. Has a capacitance and inductance effects.
4. Has a characteristic impedance 50 Ω to 100 Ω.
5. Sealed by a PVC insulator to reduce weight.
6. Limited distance to carry the data.

2.2.2 Wireless communications

Wireless communication is communication system that does not use physical wire. This communication also serves the purpose to send and receive data from far distance. The distance is not a problem because there are many routers will help to route the signals from one point to another point in the network until the signals terminated at their destinations. Wireless communication can be divided into two types. Communication using radio waves and communication using light.

Communication using radio waves is refers to using electromagnetic waves or electric fields to communicate each other. This radio waves are generated by a small antenna, which installed on every wireless communication devices. Antenna

responsible transmit and receive the radio waves which content information. Two types of antennas usually employed in wireless communications, one is element antennas and second one is patch antenna [16]. As shows the figures 2.2.

(a) monopole antenna

(b) Dipole antenna

(c) Yagi antenna

(d) Dish antenna

Figure 2.2: Element antennas [17].

The element antennas are bulky and most of them operates in low frequency. Only few are operate in high frequency like the dish antenna. The element antennas further divided into four types: wide band, narrow band, high gain and low gain. The element antennas have the following characteristics:

1. Operate in medium to high frequency
2. Installed outdoor or indoor

3. Position is fixed unless in the cell phone
4. High efficiency
5. Characteristic impedance nearly 50 Ω
6. Support LTE operations

The patch antenna on the other hand is a small size antenna that build into a mobile communication devices. This patch antenna also build in a communication device, especially it build on to the printed circuit board. Most of patch antennas are operate in microwave range. Example of patch antennas are shown in Figure 2.3.

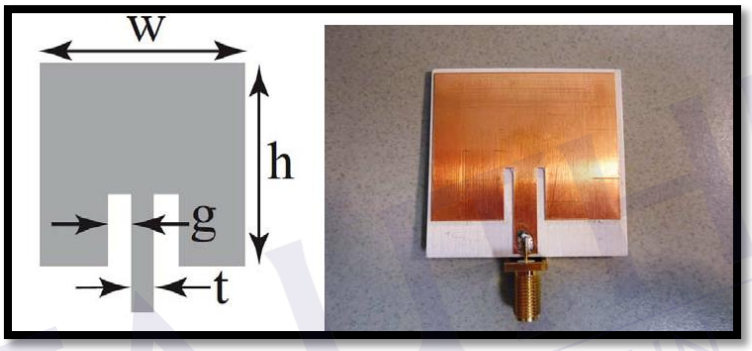
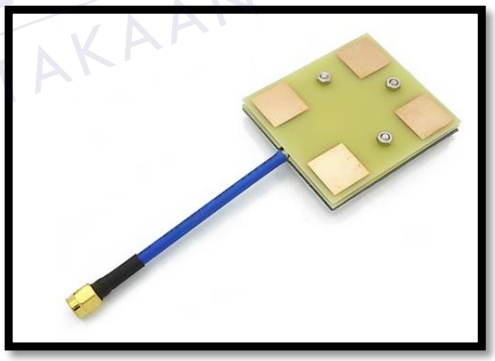


Figure (2.3) Rectangular patch antenna [18].



(b) Rectangular array antenna

Figure 2.3: Patch antenna

The wireless communications not only depends on the antennas, but also depends the following parameters:

1. Transmit power
2. Environment phenomena
3. Impedance matching

The transmit power of a transmitter is given by [19] :

$$P_{transmit} = \frac{G_t \lambda^2}{(4\pi R)^2} \quad (2.1)$$

Where G_t = transmit antenna gain

λ = wavelength

R = distance between the sensor node and the gateway

The receive power from the gateway is:

$$P_{receive} = \frac{P_{transmit} G_r G_t \lambda^2}{(4\pi R)^2} \quad (2.2)$$

Where G_r is the receive antenna gain.

Clearly it is seen that from the power transmission and reception, the antenna gain plays an important role.

The wireless communication also depending on the medium around the environment. The medium although is an air, but the radio waves will suffer from six phenomena during the propagation. These six phenomena are [20]:

a) Reflections
b) Refractions
c) Diffractions
d) Absorptions
e) Scattering
f) Tunnelling

Reflection is a phenomena where the radio waves (incident waves) hit on the object and part of it (reflected waves) reflected from the object. The reflection of the waves can be perfect or none perfect. The perfection of reflection depending the nature appearance of the object. If the object is a glass or having a smooth or flat surface, then the reflection is perfect. The perfect reflection of waves often will have incident angel,

θi equal to the reflected angle, θ_r. A normal line where it cause the reflection happen will be tangent perpendicular to the surface of the perfect reflection surface. Figure 2.4 shows the perfect and imperfect reflection of radio waves.

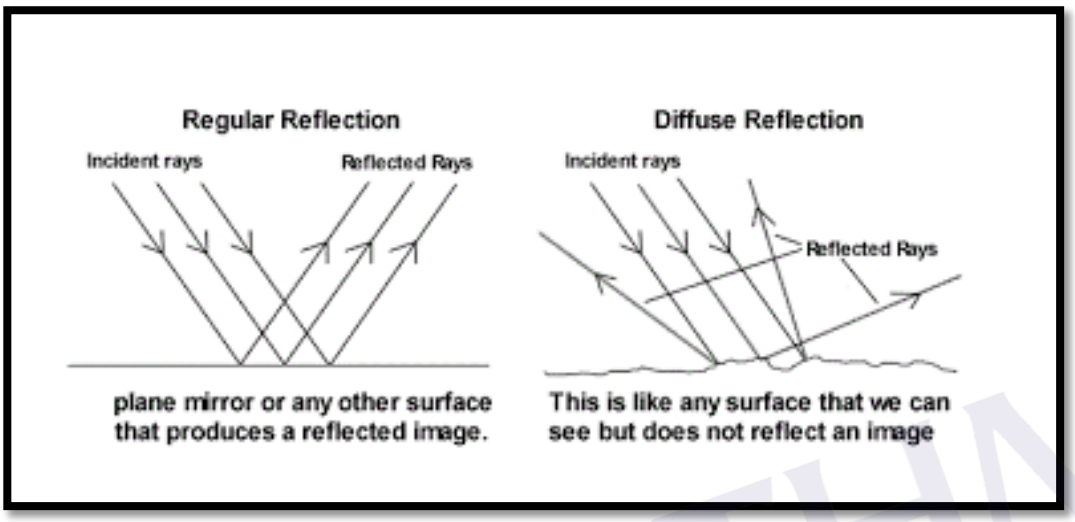


Figure 2.4: Reflection of the radio waves [21].

For imperfect reflection, there will be multiple reflections and the waves randomly reflected with no direction. The imperfect reflection happens because the surface of the object is not smooth (see Figure 2.4 (b)). The imperfect reflection reflection can cause multipath propagation of the waves. Thus, when multipath propagation of the waves meet at the receiver point, the waves can cancel each other or superimposed each other depends on the phase changes of the waves.

Refraction is another phenomena where the waves is refracted when penetrate through an object. The refraction will cause the wave's speed slow down and the the direction could be miss. Depending on the object's thickness, refraction can be increased if the thickness of an object increase. Figure 2.5 shows the refraction of the waves.

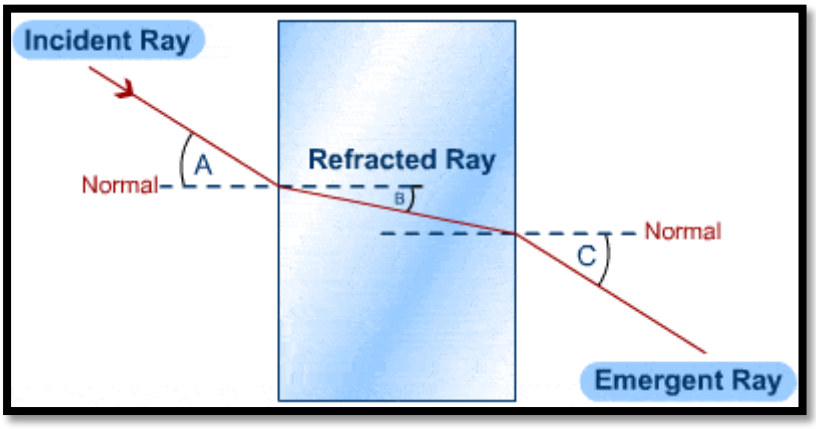


Figure 2.5: The refraction of waves using ray as an example [22].

Refraction also will cause the waves attenuated or reduced. When this happen, then we said that the wave is absorbed by the object. Thus, absorption is a phenomena where the wave's amplitude is being reduced. After portions of the waves being absorbed, the waves come out from the object will have the amplitude less than the incident wave or incident ray. The absorption of waves depends very much on the nature materials. Some materials can absorb the waves more than the other materials. The diffraction is a phenomena where the waves is diffracted at the edge of an object. The diffraction similar to the reflection except it happen at the edge of an object. Figure 2.6 shows the diffraction of radio waves [23].

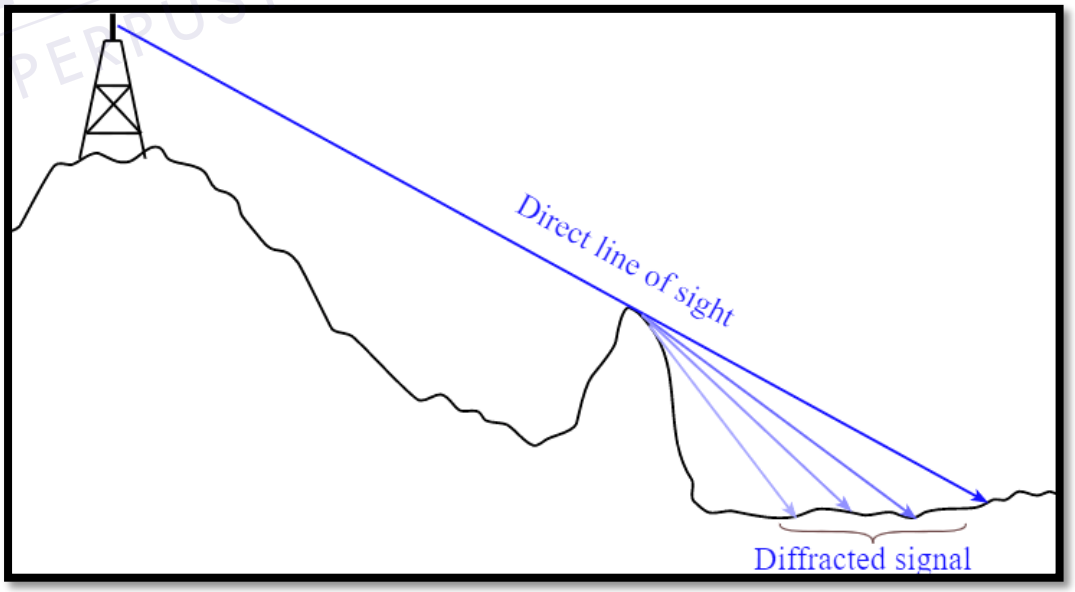


Figure 2.6: Diffraction of waves [24]

Diffraction of waves also can cause multipath propagation and scattering of the waves. This is usually happen quite often inside the building where inside the building consists of many objects.

Scattering is a phenomena where the waves scatter around the environment due to diffraction and reflection. Scattering of waves could be a good and bad depending on the receiver position. Sometimes, in scattering, multiple user terminals can get the signals. On the other hand, if scattering happens for the wireless sensor nodes located at far distance, then those nodes will not able to detect the waves.

Scattering could be considered part of the radio wave energy wasting. Thus, when designer want to position the transmitter, he or she has to consider the nodes at far distances. Bringing the nodes as closed to the transmitter as possible will remove the scattering of waves. Thus, this can achieve energy saving [25]. Another phenomena called tunnelling also quite often happen in the indoor propagation of the radio waves. Tunnelling can be understood if refers to the diagram shown in Figure 2.7.

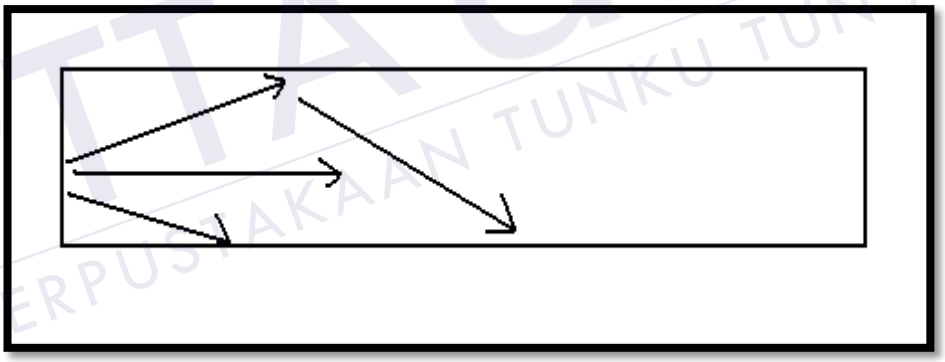


Figure 2.7: Tunnelling of radio waves [26].

Tunnelling causes the waves propagate along the tunnel and reach the destination. In tunnelling, there are reflection, diffraction and refraction of waves happen. Sometimes an echo frequency also could happen. This is depends on the nature of the walls and objects around the environments.

REFERENCES

[1] Bergen, Arthur. R and Vittal. M, "The Security Implementation System in WSN Network to Avoid Malicious Attack", *IEEE Trans on Advanced Communications*, Vol. 12, Issue 5, pp. 1 - 13, 2014.

[2] El-Waray and Glover.I, "Network Security using Frequency Hopping", *IEEE Trans on Telecommunication*, Vol. 33, Issue 1, pp. 89 - 100, 2015.

[3] Grainger, John.K and Ling.K.S, "Security System in Wireless HAN Network", *International Journal on Engineering and Technology*, Vol. 15, Issue 8, pp. 10 20, 2016.

[4] Magid, Leonard. M, "Introduction to HAN Network for Smart House System", *IEEE Trans on Electronic Communications*", Vol. 64, Issue 12, pp. 3 - 20, 2017.

[5] Mohan, Ned and Tore.M, "Wireless Network Security using CDMA Scheme", *International Journal on Engineering and Security*, Vol. 32, Issue 100, pp. 23 – 76, 2018.

[6] Undelead, Robbin. T and Weedy.R, "Introduction to Frequency Hopping for Security", *IEEE Trans on Wireless Communications*, Vol. 85, Issue 45, pp. 5 - 23, 2017.

[7] Chong Yi, Laura. J and Thing.S, "Methods of Modelling the CDMA and Frequency Hopping for Network Security", *IEEE Trans on Security of Wireless Communications*, Vol. 22, Issue 13, pp. 69 - 81, 2018.

[8] Candra.K and Chong Wen Tze, "Implementation of CDMA Using MATLAB Coding", *International Journal on Engineering and Technology*, Vol. 88, Issue 73, pp. 90 - 100,
2017.

[9] William.P and Freris.L, "Modelling and Simulation of CDMA Using MATLAB", *International Journal on Engineering and Technology*, Vol. 77, Issue 12, pp. 70 - 100, 2016.

[10] Sato.N and Sttor.R, "Using CDMA Frequency Hopping to Prevent Third Party

Attack", *IEEE Trans on Electronic Communications*, Vol. 18, Issue 17, pp. 89 - 98, 2018.

[11] Carson.J, Brown H.E and Ting.T, "Basic Understanding of Visual Basic Used in Engineering", *International Journal on Engineering and Technology*, Vol. 124, Issue 86, pp. 45 - 100, 2018.

[12] Adair.E.R and Booth.E.S, "The Advantages of Using Simulation Tools", *International Journal on Engineering and Technology*, Vol. 66, Issue 34, pp. 105 - 114, 2016.

[13] D.N. Rarn and M. Ramanoorthy, Introduction to Digital Communication, McGraw-Hill, New York, 2014.

[14] T.F. Gallen and M. Chamia, Fundamental of Fibre Optic, Prentice-Hall, New York, 2015.

[15] W.J. Smolinski, G.D. Rockgiller and Ting Sii Ying, "The Characteristics of Copper Wires for High Frequency Communications", *IEEE Trans on Telecommunications*, Vol. 3, Issue 14, pp. 5 - 20, 2016.

[16] M.M.Chen and Donita.K, Antennas, Pearson, New York, 2017.

[17] Y. Miki, Y. Sano and J.J. Makino, Applied Electromagnetism and Antennas, Oxford Press, London, 2015.

[18] A.G. Phadke, Introduction to Antennas, Longman, New York, 2016.

[19] P.K. Dash, H.P. Khinda and A.T. John, "Comparison of Outdoor and Indoor Radio Waves Propagations, *International Journal on Engineering*, Vol. 45, Issue 34, pp. 22 - 36, 2016.

[20] S. Liberman and J. Rushton, Radio Waves Propagations, Prentice-Hall, New York, 2016.

[21] R.A. Larner, L.M. Wedepol and C. Adamson, "Empirical Study on Radio Wave Propagations", *IEEE Trans on Antenna and Propagations*, Vol. 78, Issue 50, pp. 10 - 30, 2017.

[22] J. Rushton and A.R. Van, Introduction to Radio Wave Propagations, McGraw-Hill, New York, 2016.

[23] C.R. Mason, B.D. Russel and T.S.M. Rao, "Modelling of Diffraction Phenomena", *IEEE Trans on Electromagnetism*, Vol. 89, Issue 45, pp. 40 - 78, 2016.

[24] S.S. Rao, Radio Frequency Communications, Pearson, New York, 2015.

[25] A.P. Muthur, R.S. Gaonker and M. Kumran, "Simulation on Scattering of 2.4

GHz", *IEEE Tans on Wireless Communications*, Vol. 90, Issue 55, pp. 37 - 67, 2017.

[26] B.Ram, Adam.S and K.K.A. Devi, "The Tunnelling Effects on the Radio Waves", *International Journal on Telecommunications*, Vol. 90, Issue 22, pp. 6 - 19, 2015.

[27] Yu cheng, D.F. Elliot and K.R. Rao, "Introduction to Computer Networks", McGraw-Hill, New York, 2016.

[28] G.D. Rat and W.W. Lewis, Basic Computer Networking, Pearson, New York, 2016.

[29] H. Cotton and M. Khalifa, "Design and Modelling of 2.4 GHz Personal Area Network", *IEEE Trans on Digital Communications*, Vol. 69, Issue 12, pp. 58 – 77, 2015.

[30] Abo bakar .A,Ali.MandHussien .M,2016

[31] W.A. Elmore and J.L. Blackbum, Introduction to Wireless Communications, McGraw-Hill, New York, 2014.

[32] Chan Chin Chin and Shelyn. Lim, Introduction Media Access Control, Pearson, New York, 2016.

[33] C.G. Dewey and S.P. Patra, Digital Communications, Longman, New York, 2015.

[34] K.parveena ,M.valamathi and R.Ravitha,2016

[35] J.A. lmlof and N.M. Anil, Basic Digital Communications, Pearson, New York, 2016.

[36] Donald.E and Helmut.H, "Simulation on WCDMA Using MATLAB", IEEE Trans on Digital Communications, Vol. 90, Issue 100, pp. 50 - 78, 2014.

[37] Arnoid. G, Advanced Communications, Longman, New York, 2017.

[38] B. Jeyasurya and W.J. Smolink, "Mathematical Analysis on OFDMA", *International Journal on Communications and Controls*, Vol. 65, Issue 36, pp. 48 - 70, 2017.

[39] H. Kudo and M.A. Baribeu, Introduction Spread Spectrum, Pearson, New York, 2016.

[40] Charles.F, Analogue and Digital Communications, Longman, New York, 2016.

[41] Donita.K, "Analysis of Frequency Hopping for Multiple Channels", *IEEE Trans on Electronic Communications*, Vol. 88, No. 14, pp. 30 - 67, 2016.

[42] Lily Chen Yew Ling, Adaptive Frequency Hopping, *IEEE Trans on Electronic Communications*, Vol. 55, Issue 44, pp. 23 - 103, 2016.

[43] Chong Kok Ming, Advanced Digital Communications, Pearson, New York, 2012.

[44] Kwong Chiew Fung, Basic Digital Communications, Longman, New York, 2015.

[45] Sukurma.H, Morden Digital Communications, Pearson, New York, 2017.

[46] Peter.E, Digital Communications and Control, Longman, New York, 2014.

[47] Pee Ah Chin and Sandra.L, "Spread Spectrum Analysis", *IEEE Trans on Communications*, Vol. 33, Issue 12, pp. 90 - 123, 2016.

[48] Jeffrey.C, "Modelling of Spread Spectrum Using MATLAB", *International Journal on Digital Communications*, Vol. 99, Issue 80, pp. 7 - 86, 2016.

[49] Sandra. L and Maggie. C, Digital Communications and Practices, McGraw-Hill, New York, 2016.